UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/637,123	08/11/2000	Ramanathan Ramanathan	042390.P9016	7337

7590 04/14/2004

Blakely Sokoloff
Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	3

DATE MAILED: 04/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/637,123	RAMANATHAN, RAMANATHAN	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 August 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 2.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-29 have been presented for examination.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 1/16/2001, has been considered by the examiner.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 12-16, and 23-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over McArdle et al., (U.S. Patent No. 6,442,686 and McArdle hereinafter) in view of Susakie et al., (U.S. Patent No. 6,253,322 and Susakie hereinafter).

Regarding claim 1, McArdle discloses a method comprising a policy administrator (i.e., server side 380):

establishing a network monitoring digital contract (i.e., email message) with a network monitoring element (i.e., policy management agent 381 and analysis engine 385), establishing a network use digital contract (i.e., email message) with a first and a

second network element (i.e., communicating to the sender and the receiver of the email message)(Col. 10, lines 22-67 and Col. 11, lines 30-67 and Col. 12, lines 1-67).

McArdle does not expressly disclose transmitting decrypting information to the network monitoring element for decrypting encrypted communications.

However, Susaki discloses

transmitting decrypting information to the network monitoring element (i.e., certificate authority 170) for decrypting encrypted communications between the first network element and the second network element (i.e., service supplying unit 130 and service receiving unit 140) per terms in the network monitoring digital contract and the network use digital contract (Col. 9, lines 60-67 and Col. 10, lines 1-65).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susakie to include transmission of encryption key as part of the digital contract with the motivation to provide for reliable electronic commerce using cryptographic technology (Susakie, Col. 1, lines 6-10).

Regarding claim 2, McArdle discloses encrypted communication between a sender, a receiver, and a policy management agent (Col. 10, lines 22-67 and Col. 11, lines 30-67 and Col. 12, lines 1-67).

McArdle does not expressly disclose transmitting decrypting information to the network monitoring element.

However, However, Susaki discloses

communicating the common key between service supplying unit and the certificate authority (Col. 9, lines 60-67 and Col. 10, lines 1-65).

transmitting decrypting information to the network monitoring element (i.e., certificate authority 170) for decrypting encrypted communications between the first network element and the second network element (i.e., service supplying unit 130 and service receiving unit 140) per terms in the network monitoring digital contract and the network use digital contract comprises the policy administrator (Col. 4, lines 33-67 and Col. 5, lines 1-67, Col. 6, lines 1-57);

receiving a request from the network monitoring element for the decrypting information, transmitting a request to the network monitoring element for the network monitoring digital contract, receiving the network monitoring digital contract from the network monitoring element (Col. 9, lines 60-67 and Col. 10, lines 1-67 and Col. 11, lines 1-7);

authenticating the received network monitoring digital contract (Col. 4, lines 33-67 and Col. 5, lines 1-67, Col. 6, lines 1-57); and

transmitting decrypting keys to decrypt the encrypted communications between the first network element (i.e., service supplying unit 130) and the second network element (i.e., service receiving unit 140) to the network monitoring element (Col. 6, lines 29-57);

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susakie to include communicating of decrypting information and authenticating the

communicated information with the motivation to provide for reliable electronic commerce using cryptographic technologies (Susakie, Col. 1, lines 5-10).

Regarding claim 3, McArdle does not expressly disclose transmitting decrypting information to the network monitoring element.

However, Susakie discloses wherein transmitting decrypting information to the network monitoring element (i.e., certificate authority 170) for decrypting encrypted communications between the first network element (i.e., service supplying unit 130) and the second network element (i.e., service receiving unit 140) per terms in the network monitoring digital contract (Col. 4, lines 33-67 and Col. 5, lines 1-67, Col. 6, lines 1-57); and

Moreover, McArdle discloses the network use digital contract comprises the policy administrator decrypting the encrypted communications between the network elements and transmitting the decrypted communications to the network monitoring element (i.e., policy management agent 381 controls all the communications between the messaging client 325 and the messaging gateway 391. Policy management agent traps the outbound message and processes it according to crypto-policy rules which has been established for the system)(Col. 11, lines 54-67 and Col. 12, lines 1-35).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susakie to include communicating of decrypting information and authenticating the

communicated information with the motivation to provide for reliable electronic commerce using cryptographic technologies (Susakie, Col. 1, lines 5-10).

Regarding claim 12, McArdle discloses a method, comprising:

establishing by a first network element (i.e., sender/email client, 325), a network use digital contract with a policy administrator (i.e., policy management agent, 381), communicating with a second network element per the terms of the network use digital contract (i.e., if the email message conforms to the rules, it then may be passed on to the messaging gateway, for transport to the intended recipient)(Col. 11, lines 30-67 and Col. 12, lines 1-35); and

logging in a secure manner, encryption and authenticating algorithms, and decryption keys used in the communication, and permitting the policy administrator access to the log to obtain the decrypting keys (Col. 12, lines 35-67 and Col. 13, lines 1-17).

Regarding claim 13, McArdle does not expressly disclose digital certificates.

However, Susaki discloses wherein establishing by a first network element (i.e., service supplying unit), a network use digital contract with a policy administrator (i.e., service receiving unit) comprises a network element:

transmitting its digital certificate, transmitting its digital signature, and receiving a copy of the network use digital contract from the policy administrator (i.e., the service

receiver 110, receives and deciphers contract information 160 using the service receiving unit 140 in step 905a)(Col. 11, lines 50-67 and Col. 12, lines 1-60).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susaki to include transmitting and receiving digital certificates between network monitoring element and the policy administrator with the motivation to achieve implementing certification and authentication services (Susaki, Col. 2, lines 44-67).

Regarding claim 14, McArdle discloses an article of manufacture comprising: a machine-readable medium (i.e., client side and server side storage) that provides instructions (i.e., Microsoft Outlook email client), that when executed by a machine, cause said machine to perform operations comprising:

establishing a network monitoring digital contract with a network monitoring element (i.e., sending email from sender's machine to the policy management agent), establishing a network use digital contract with a first and a second network element i.e., communicating with sender and/receiver)(Col. 11, lines 30-67 and Col. 12, lines 1-67).

McArdle does not expressly disclose transmitting decrypting information to the network monitoring element to decrypt encrypted communication between first and second network elements.

However, Susakie discloses:

transmitting decrypting information to the network monitoring element for decrypting encrypted communications between the first network element (i.e., service supplying unit 130) and the second network element (i.e., service receiving unit 140) per terms in the network monitoring digital contract and the network use digital contract (Col. 10, lines 35-67 and Col. 11, lines 1-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susakie to include communicating decrypting information for decrypting encrypted communications with the motivation to provide for reliable electronic commerce using cryptographic technologies (Susakie, Col. 1, lines 5-10).

Regarding claim 15, McArdle does not expressly disclose transmitting decrypting information to the network monitoring element to decrypt encrypted communication between first and second network elements.

However, Susakie discloses wherein said instructions for transmitting decrypting information to the network monitoring element for decrypting encrypted communications between the first network element and the second network element per terms in the network monitoring digital contract and the network use digital contract, include further instructions to direct the policy administrator

to receive a request from the network monitoring element for the decrypting information, to receive the network monitoring digital contract from the network monitoring element (Col. 9, lines 60-67 and Col. 10, lines 1-67 and Col. 11, lines 1-7);

to authenticate the network monitoring digital contract (Col. 4, lines 33-67 and Col. 5, lines 1-67, Col. 6, lines 1-57); and

to transmit decrypting information, including decrypting keys needed to decrypt the encrypted communications between the network elements (i.e., service supplying unit 130) and the second network element (i.e., service receiving unit 140) to the network monitoring element (Col. 6, lines 29-57);

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susakie to include communicating of decrypting information and authenticating the communicated information with the motivation to provide for reliable electronic commerce using cryptographic technologies (Susakie, Col. 1, lines 5-10).

Regarding claim 16, McArdle does not expressly disclose wherein said instructions for transmitting decrypting information to the network monitoring element for decrypting encrypted communications between the first network element and the second network element per terms in the network monitoring digital contract and the network use digital contract include further instructions.

However, Susakie wherein said instructions for transmitting decrypting information to the network monitoring element for decrypting encrypted communications between the first network element and the second network element per terms in the network monitoring digital contract and the network use digital contract (Col. 10, lines 35-67 and Col. 11, lines 1-25) include further instructions:

to decrypt the encrypted communications between the network elements (Col 10, lines 25-67 and Col. 11, lines 1-7); and

to transmit the decrypted communications to the network monitoring element (Col. 6, lines 29-57).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susakie to include communicating decrypting information for decrypting encrypted communications with the motivation to provide for reliable electronic commerce using cryptographic technologies (Susakie, Col. 1, lines 5-10).

Regarding claim 23, McArdle discloses an article of manufacture comprising: a machine-readable medium that provides instructions, that when executed by a machine, cause said machine to perform operations comprising:

establishing by a first network element (i.e., sender/email client, 325), a network use digital contract with a policy administrator (i.e., policy management agent, 381), communicating with a second network element per the terms of the network use digital contract (i.e., if the email message conforms to the rules, it then may be passed on to the messaging gateway, for transport to the intended recipient)(Col. 11, lines 30-67 and Col. 12, lines 1-35);

logging in a secure manner, encryption and authenticating algorithms, and decryption keys used in the communication, and permitting the policy administrator

access to the log to obtain the decrypting keys (Col. 12, lines 35-67 and Col. 13, lines 1-17); and

permitting the policy administrator access to the log to obtain the decrypting keys (Col. 6, lines 20-67 and Col. 7, lines 1-67 and Col. 8, lines 1-57).

Regarding claim 24, McArdle does not expressly disclose communication of a digital contract.

However, Susaki discloses wherein establishing by a first network element (i.e., service supplying unit), a network use digital contract with a policy administrator (i.e., service receiver) comprises a network element:

transmitting its digital certificate, transmitting its digital signature, and receiving a copy of the network use digital contract from the policy administrator (i.e., the service receiver 110, receives and deciphers contract information 160 using the service receiving unit 140 in step 905a)(Col. 11, lines 50-67 and Col. 12, lines 1-60).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susaki to include transmitting and receiving digital certificates between network monitoring element and the policy administrator with the motivation to achieve implementing certification and authentication services (Susaki, Col. 2, lines 44-67).

Claims 4-11, and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over McArdle et al., (U.S. Patent No. 6,442,686 and McArdle hereinafter)

and Susakie et al., (U.S. Patent No. 6,253,322 and Susakie hereinafter), in view of Andrews et al., (U.S. Patent No. 6,324,645 and Andrews hereinafter).

The teachings of McArdle and Susakie have been discussed previously.

Regarding claim 4, McArdle or Susakie does not expressly disclose the use of digital certificate and digital signature for authentication.

However, Andrews disclose wherein establishing a network monitoring digital contract with a network monitoring element (i.e., a user) comprises:

receiving a network monitoring element's digital certificate, authenticating the network monitoring element's digital certificate (Col. 9, lines 22-67 and Col. 10, lines 1-53);

receiving a network monitoring element's digital signature, authenticating the network monitoring element's digital signature (Col. 4, lines 50-67 and Col. 5, lines 1-11);

writing contract terms in an electronic document (i.e., the digital certificate 200 uses the X.509 format and includes a serial number 202, the CA's distinguished name 204, the user 102's distinguished name 206, a period of validity 208, the user 102's public key 210, possibly digital certificate extensions 212, and the CA's digital signature 214)(Col. 7, lines 37-67 Col. 8, lines 1-67 and Col. 9, lines 1-59 and Col. 10, lines 19-52 and Col. 11, lines 34-50).

Furthermore, Susakie discloses:

writing the network element's digital certificate and the network element's digital signature in the electronic document (Col. 12, lines 45-67 and Col. 13, lines 1-10);

writing a digital certificate of the policy administrator and a digital signature of the policy administrator in the electronic document; and transmitting a copy of the electronic document to the network element (Col. 13, lines 10-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include computer-implemented techniques based on digital certificates with the motivation to efficiently allow multiple users to share a public key management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Regarding claim 5, McArdle or Susakie does not expressly disclose writing of the contract terms in an electronic document.

However, Andrews discloses wherein writing contract terms in an electronic document comprises:

writing an effective date and time of the network monitoring digital contract, writing a time period during which the network monitoring digital contract is valid (i.e., period of validity, Fig. 2, element 208)(Col. 6, lines 18-35 and Col. 9, lines 22-59).

specifying the decrypting information (i.e., user public key, 210), including decrypting keys the network monitoring element is to receive (Col. 9, lines 22-59).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include digital certificates including date and time validity information as well as decrypting information with the motivation to provide for a better security (Andrews, Col. 6, lines 25-35).

Regarding claim 6, McArdle or Susakie does not expressly disclose digital certificates and signatures.

However, Andrews discloses wherein establishing a network use digital contract with each network element comprises:

receiving a network monitoring element's digital certificate, authenticating the network monitoring element's digital certificate (Col. 9, lines 22-67 and Col. 10, lines 1-53);

receiving a network monitoring element's digital signature, authenticating the network monitoring element's digital signature (Col. 4, lines 50-67 and Col. 5, lines 1-11);

writing contract terms in an electronic document (i.e., the digital certificate 200 uses the X.509 format and includes a serial number 202, the CA's distinguished name 204, the user 102's distinguished name 206, a period of validity 208, the user 102's public key 210, possibly digital certificate extensions 212, and the CA's digital signature 214)(Col. 7, lines 37-67 Col. 8, lines 1-67 and Col. 9, lines 1-59 and Col. 10, lines 19-52 and Col. 11, lines 34-50).

Furthermore, Susakie discloses:

writing the network element's digital certificate and the network element's digital signature in the electronic document (Col. 12, lines 45-67 and Col. 13, lines 1-10);

writing a digital certificate of the policy administrator and a digital signature of the policy administrator in the electronic document; and transmitting a copy of the electronic document to the network element (Col. 13, lines 10-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include computer-implemented techniques based on digital certificates with the motivation to efficiently allow multiple users to share a public key management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Regarding claim 7, McArdle or Susakie does not expressly disclose writing of the contract terms in an electronic document.

However, Andrews discloses wherein writing contract terms in an electronic document comprises:

writing an effective date and time of the network use digital contract (i.e., period of validity, Fig. 2, element 208)(Col. 6, lines 18-35 and Col. 9, lines 22-59); and

specifying the decrypting information (i.e., user public key, 210), including decrypting keys the policy administrator obtains from the network element (Col. 9, lines 22-59).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include digital certificates including date and time validity information as well as decrypting information with the motivation to provide for a better security (Andrews, Col. 6, lines 25-35).

Regarding claim 8, McArdle discloses that the PGP runtime engine builds a status list for the message (Col. 12, lines 35-67 and Col. 13, lines 1-18).

McArdle or Susakie does not expressly disclose transmitting the network policy to network elements.

However, Andrews discloses further comprising:

establishing a network policy (Col. 1, lines 65-67 and Col. 2, lines 1-67).

transmitting the network policy (i.e., digital certificate) to network elements (i.e., users of the network)(Col. 6, lines 18-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include computer-implemented techniques (i.e., network policies) based on digital certificates with the motivation to efficiently allow multiple users to share a public key management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Regarding claim 9, McArdle or Susakie does not expressly disclose a network monitoring element establishing a network monitoring digital contract with a policy administrator.

However, Andrews discloses comprising a network monitoring element:

establishing a network monitoring digital contract (i.e., digital certificate) with a policy administrator (i.e., certification authority, CA)(Col. 10, lines 19-67 and Col. 12, lines 24-67);

transmitting a request to monitor encrypted communications between network elements, transmitting the network monitoring digital contract (i.e., authenticating the user to access and use the appropriate public key to decrypt the encrypted message by issuing and transmitting a digital certificate)(Col. 4, lines 35-67); and

receiving decrypting information (i.e., digital certificate including public key, 210), including decrypting keys from the policy administrator (i.e., certification authority) for decrypting encrypted communications between a first network element and a second network element per the terms in the network monitoring digital contract (i.e., digital certificate contains information a user's privileges such as encrypting decrypted messages)(Col. 9, lines 22-58).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include computer-implemented techniques (i.e., network policies) based on digital certificates and the capability to monitor encrypted communications with the motivation to efficiently allow multiple users to share a public

key management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Regarding claim 10, McArdle does not expressly disclose wherein receiving decrypting information from the policy administrator for decrypting encrypted communications.

However, Susakie discloses wherein receiving decrypting information from the policy administrator for decrypting encrypted communications between a first network element (i.e., service supplying unit 130) and a second network element (i.e., service receiving unit 140) per the terms in the network monitoring digital contract comprises receiving from the policy administrator decrypted communications after the policy administrator (i.e., certificate authority 170) decrypts the encrypted communications between the network elements (Col. 4, lines 33-67 and Col. 5, lines 1-67, Col. 6, lines 1-57); and

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susakie to include communicating decrypting information for decrypting encrypted communications with the motivation to provide for reliable electronic commerce using cryptographic technologies (Susakie, Col. 1, lines 5-10).

Regarding claim 11, McArdle does not expressly disclose communication of digital certificate between network monitoring element and the policy administrator.

However, Susaki discloses wherein establishing a network monitoring digital contract with a policy administrator (i.e., service receiver unit) comprises a network monitoring element (i.e., certificate authority 170):

transmitting its digital certificate to the policy administrator (i.e., service receiving unit), transmitting its digital signature to the policy administrator (i.e., service receiving unit)(Col. 5, lines 55-67); and

receiving a copy of the network monitoring digital contract (i.e., digital certificate) from the policy administrator (i.e., certificate authority 170)(Col. 12, lines 24-67 and Col. 13, lines 1-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Susaki to include transmitting and receiving digital certificates between network monitoring element and the policy administrator with the motivation to achieve implementing certification and authentication services (Susaki, Col. 2, lines 44-67).

Regarding claims 17 and 18, McArdle does not expressly disclose the communication of digital certificates and digital signatures.

However, Andrews discloses wherein said instructions establishing a network monitoring digital contract between a policy administrator (i.e., certificate authority) and a network monitoring element (i.e., user) include further instructions

to receive a network monitoring element's digital certificate and digital signature, and to authenticate the network monitoring element's digital certificate and digital

signature (Col. 4, lines 50-67 and Col. 5, lines 1-11 and Col. 9, lines 22-67 and Col. 10, lines 1-53);

to specify a time period during which the network monitoring digital contract is valid (i.e., period of validity, Fig. 2, element 208)(Col. 6, lines 18-35 and Col. 9, lines 22-59);

to write the contract terms, including an effective date and time of the network monitoring digital contract (i.e., the digital certificate 200 uses the X.509 format and includes a serial number 202, the CA's distinguished name 204, the user 102's distinguished name 206, a period of validity 208, the user 102's public key 210, possibly digital certificate extensions 212, and the CA's digital signature 214), and to specify the decrypting information, including decrypting keys the network monitoring element is to obtain in an electronic document (Col. 9, lines 22-59);

Furthermore, Susakie discloses:

to write the network element's digital certificate and the network element's digital signature in the electronic document (Col. 12, lines 45-67 and Col. 13, lines 1-10);

to write a digital certificate of the policy administrator and a digital signature of the policy administrator in the electronic document, and to transmit a copy of the electronic document to the network element (Col. 13, lines 10-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include computer-implemented techniques based on digital certificates with the motivation to efficiently allow multiple users to share a public key

management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Regarding claim 19, McArdle discloses that the PGP runtime engine builds a status list for the message (Col. 12, lines 35-67 and Col. 13, lines 1-18).

McArdle or Susakie does not expressly disclose transmitting the network policy to network elements.

However, Andrews discloses further comprising:

to establish a network policy (Col. 1, lines 65-67 and Col. 2, lines 1-67).

to transmit the network policy (i.e., digital certificate) to network elements (i.e., users of the network)(Col. 6, lines 18-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Susakie with the teachings of Andrews to include computer-implemented techniques (i.e., network policies) based on digital certificates with the motivation to efficiently allow multiple users to share a public key management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Claims 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over McArdle et al., (U.S. Patent No. 6,442,686 and McArdle hereinafter), in view of Andrews et al., (U.S. Patent No. 6,324,645 and Andrews hereinafter).

Regarding claim 20, McArdle does not expressly disclose a network monitoring element establishing a network monitoring digital contract with a policy administrator.

However, Andrews discloses an article of manufacture comprising: a machine-readable medium that provides instructions, that when executed by a machine, cause said machine to perform operations comprising:

establishing a network monitoring digital contract (i.e., digital certificate) with a policy administrator (i.e., certification authority, CA)(Col. 10, lines 19-67 and Col. 12, lines 24-67);

transmitting a request to monitor encrypted communications between network elements, transmitting the network monitoring digital contract (i.e., authenticating the user to access and use the appropriate public key to decrypt the encrypted message by issuing and transmitting a digital certificate)(Col. 4, lines 35-67); and

receiving decrypting information (i.e., digital certificate including public key, 210), including decrypting keys from the policy administrator (i.e., certification authority) for decrypting encrypted communications between a first network element and a second network element per the terms in the network monitoring digital contract (i.e., digital certificate contains information a user's privileges such as encrypting decrypted messages)(Col. 9, lines 22-58).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Andrews to include computer-implemented techniques (i.e., network policies) based on digital certificates and the capability to monitor encrypted communications with the

motivation to efficiently allow multiple users to share a public key management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Regarding claim 21, McArdle does not expressly disclose wherein said instructions for receiving decrypting information from the policy administrator for decrypting encrypted communications between a first network element and a second network element per the terms in the network monitoring digital contract include further instructions to receive from the policy administrator decrypted communications after the policy administrator decrypts the encrypted communications between the network elements.

However, Andrews discloses wherein said instructions for receiving decrypting information (i.e., digital certificate including public key, 210) from the policy administrator (i.e., certification authority) for decrypting encrypted communications between a first network element and a second network element per the terms in the network monitoring digital contract include further instructions to receive from the policy administrator decrypted communications after the policy administrator decrypts the encrypted communications between the network elements (i.e., digital certificate contains information a user's privileges such as encrypting decrypted messages)(Col. 9, lines 22-58).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings

of Andrews to include computer-implemented techniques (i.e., network policies) based on digital certificates and the capability to monitor encrypted communications with the motivation to efficiently allow multiple users to share a public key management infrastructure, while simultaneously managing the risk associated with such sharing (Andrews, Col. 3, lines 12-20).

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over McArdle et al., (U.S. Patent No. 6,442,686 and McArdle hereinafter) and Andrews et al., (U.S. Patent No. 6,324,645 and Andrews hereinafter), in view of Susakie et al., (U.S. Patent No. 6,253,322 and Susakie hereinafter).

The teachings of McArdle and Andrews have been discussed previously.

Regarding claim 22, McArdle or Andrews does not expressly disclose communication of digital certificate between network monitoring element and the policy administrator.

However, Susaki discloses wherein establishing a network monitoring digital contract with a policy administrator (i.e., service receiver unit) comprises a network monitoring element (i.e., certificate authority 170):

to transmit its digital certificate to the policy administrator (i.e., service receiving unit), to transmit its digital signature to the policy administrator (i.e., service receiving unit)(Col. 5, lines 55-67); and

to receive a copy of the network monitoring digital contract (i.e., digital certificate) from the policy administrator (i.e., certificate authority 170)(Col. 12, lines 24-67 and Col. 13, lines 1-20).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle and Andrews with the teachings of Susaki to include transmitting and receiving digital certificates between network monitoring element and the policy administrator with the motivation to achieve implementing certification and authentication services (Susaki, Col. 2, lines 44-67).

Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over McArdle et al., (U.S. Patent No. 6,442,686 and McArdle hereinafter) in view of Dyksterhouse et al., (U.S. Patent No. 6,336,186 and Dyksterhouse hereinafter).

Regarding claim 25, McArdle discloses an apparatus comprising:

a receiver to receive a request for decrypting information, and to receive a network monitoring digital contract from a network monitoring element (i.e., server side , 380, receives sender's email message)(Col. 8, lines 57-67 and Col. 9, lines 1-25);

McArdle does not expressly disclose a multiprocessor coupled to the receiver and a memory to process the encrypted content.

However, Dyksterhouse discloses a microprocessor (i.e., certificate server, 381) communicatively coupled to the receiver (i.e., server side, 380) and a memory (i.e., certificate database, 385) to authenticate the network monitoring digital contract (i.e.,

certificate server allows clients to submit keys to the database based on a set of policy constraints so that they may be retrieved and used as decrypting information)(Col. 8, lines 9-63);

a transmitter communicatively coupled to said microprocessor and memory to transmit a network policy and decrypting information, including decrypting keys to decrypt encrypted communications between network elements (i.e., ability to replicate database entries to multiple servers that are automatically updated to reflect the contents of the primary server)(Col. 8, lines 9-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Dyksterhouse to include a microprocessor coupled to a receiver and a transmitter coupled to a microprocessor and a memory with the motivation to encrypt/decrypt data and verify digital signatures (Dyksterhouse, Col. 4, lines 15-20).

Regarding claim 26, McArdle does not expressly disclose a multiprocessor coupled to the receiver and a memory to process the encrypted content.

However, Dyksterhouse discloses wherein the microprocessor retrieves from the memory decrypting information including decrypting keys, to decrypt the encrypted communications between the network elements and to transmit the decrypted communications to the network monitoring element (i.e., decryption information is retrieved from the database to decrypt encrypted information through flexible key

retrieval that support searches on multiple key attributes such as the key type)(Col. 8, lines 9-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Dyksterhouse to include a microprocessor coupled to a receiver and a memory with the motivation to encrypt/decrypt data and verify digital signatures (Dyksterhouse, Col. 4, lines 15-20).

Regarding claim 27, McArdle does not expressly disclose a multiprocessor coupled to the receiver and a memory to process the encrypted content.

However, Dyksterhouse discloses wherein the microprocessor retrieves from a network element decrypting information including decrypting keys and the transmitter transmits the decrypting information to the network monitoring element (i.e., at the server side 380 a certificate server 381 stores and maintains certificate information in a certificate database 385 and clients submit and retrieve keys from the database)(Col. 8, lines 9-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of McArdle with the teachings of Dyksterhouse to include a microprocessor coupled to a receiver and a memory with the motivation to encrypt/decrypt data and verify digital signatures (Dyksterhouse, Col. 4, lines 15-20).

Claims 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Susakie et al., (U.S. Patent No. 6,253,322 and Susakie hereinafter) in view of Dyksterhouse et al., (U.S. Patent No. 6,336,186 and Dyksterhouse hereinafter).

Regarding claim 28, Susakie discloses an apparatus comprising:

a receiver to receive a network monitoring digital contract, and decrypting information, including decrypting keys from a policy administrator, said receiver to receive encrypted communications between a first network element and a second network element (i.e., the service receiver 110, receives and deciphers contract information 160, using the service receiving unit 140, in step 905a)(Col. 11, lines 50-67 and Col. 12, lines 1-60);

Susakie does not expressly disclose a multiprocessor coupled to the receiver and a memory to process the encrypted content.

However, Dyksterhouse discloses a microprocessor (i.e., certificate server, 381) communicatively coupled to the receiver and a memory, said memory (i.e., certificate database, 385) to store the network monitoring digital contract, and to use the decrypting information, including the decrypting keys to decrypt the encrypted communications between the first and the second network element (i.e., certificate server allows clients to submit keys to the database based on a set of policy constraints so that they may be retrieved and used later on as decrypting information)(Col. 8, lines 9-63);

a transmitter communicatively coupled to the microprocessor and the memory (i.e., certificate database, 385) to transmit a request to the policy administrator for the decrypting information (i.e., keys), including the decrypting keys to decrypt the encrypted communications between the first and the second network element, and to transmit the network monitoring digital contract to the policy administrator (i.e., certificate server allows clients to retrieve keys from the database based on a set of policy constraints)(Col. 8, lines 9-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Susakie with the teachings of Dyksterhouse to include a microprocessor coupled to a receiver and a transmitter coupled to a microprocessor with the motivation to encrypt/decrypt data verify digital signatures (Dyksterhouse, Col. 4, lines 15-20).

Regarding claim 29, Susakie discloses wherein the receiver receives decrypted communications from the policy administrator (Col. 11, lines 50-67 and Col. 12, lines 1-60).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Chandersekaran et al., (U.S. Patent No. 6,058,188),

Gressel et al., (U.S. Patent No. 5,852,665),

Ganesan et al., (U.S. Patent No. 5,535,276),

Romeny et al., (U.S. Patent No. 6,085,322), and

Nemovicher, (U.S. Publication No. 2002/0007453).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Technology Center 2100
March 17, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100